

**IN THE OFFICE OF THE ADJUDICATING OFFICER OF JUDICATURE AT
CHENNAI**

Thiru P.W.C.Davidar, I.A.S., Adjudicating Officer /
Principal Secretary to Government, Information Technology Department,
Government of Tamil Nadu

CIVIL JURISDICTION

PETITION NO. 3 OF 2011

Dated 16th May 2011

Shri Thomas Raju

..... Petitioner

Versus

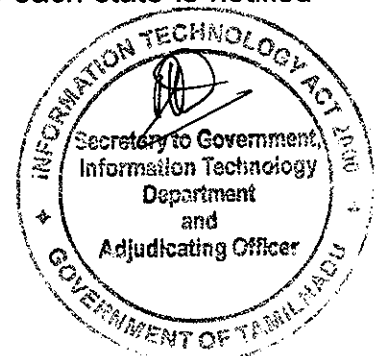
The Branch Manager,
ICICI Bank,
A -78, Plot No.3211, Third Avenue,
Anna Nagar,
Chennai-102.

& Others

.....Respondent

JUDGMENT

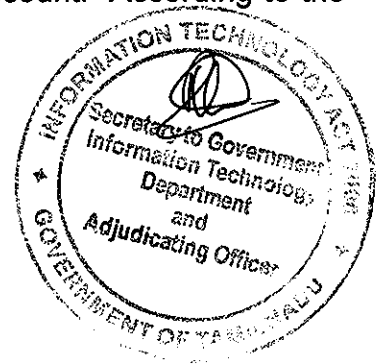
1. This is the proceedings of an application filed by the petitioner for Adjudication under section 46 of the Information Technology Act, 2000. In a follow up to the IT Act of 2000, under powers conferred by the Act, the Government of India have issued IT rules (certifying authorities) 2000, Cyber Regulations Appellate Tribunal Rules, 2000 and other rules inclusive of Notification No. GSR 220 (E), dated 17.3.2003 and 240(E) dated 25.3.2003 by which the Principal Secretary to Information Technology of each state is notified



as the Adjudication Officer under the IT Act, 2000. Consequent on the notification issued by the Government of India, the State Government has appointed the Principal Secretary to Government, Information Technology Department as the Adjudicating Officer for the State. Further, section 46 subsection (5) of the IT Act also states that every Adjudicating Officer shall have the powers of the civil court and all proceedings before the Adjudicating Officer shall be deemed to be judicial proceedings within the meaning of section 193 and 228 of the India Penal Code. In keeping with the basic principles of natural justice and reasonable opportunity by which detailed hearings were held in which both parties i.e., the petitioner and the respondent were provided with equal and adequate opportunities to present and defend their case. Following the completion of hearing and submission of affidavits and counter affidavits, the conclusion is being arrived at and the judgement being delivered herein.

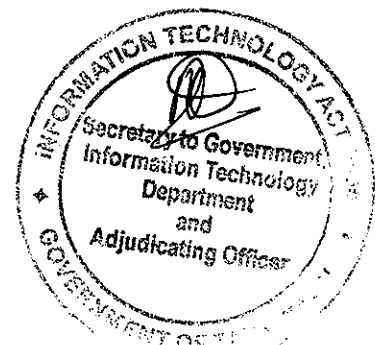
Petitioner:

2. The petitioner is working in the Information Technology sector in a private Company and during the happening of the incident complained about in this case incident, was staying in California, USA. His current residential address is 1D, Akshaya Flats, Thirukkural Street Extn., SBI Colony, Chitlapakkam, Chennai-600 064. The petitioner maintained a Savings Bank Account No.602701509178 at Anna Nagar Branch of ICICI Bank. On the 6th April, 2010, his account was debited for an amount of Rs. 1 lac and on 7th April, 2010 for Rs.62,800/- from the above mentioned Savings Bank Account. According to the



petitioner, these transactions were not authorized by him and he was not aware as to how these transactions took place. Following this incident, he registered a complaint with the ICICI helpdesk which was recorded as SR 137849004. A police complaint was also registered under Ref. No.410CHI95 which was then forward to the Cyber Cell. On 14th April, 2010, a formal complaint was made to ICICI Bank in the customer dispute form and several e-mail complaints were made to different officials of the ICICI Bank.

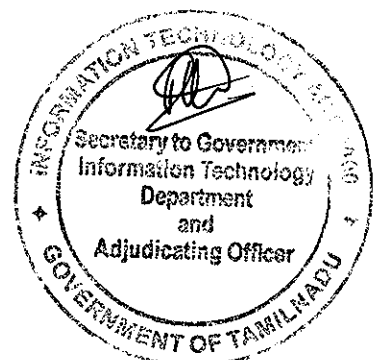
3. The petitioner submitted that he had always accessed his internet banking account through a secured virtual private network and had never compromised his password nor accessed his account from an unsecured network such as the cyber cafe etc. Also, that he had registered the mobile number of 9962546471 originally which had been changed later to that of the current mobile No.8939922880 which was registered with the account and that on June 12, 2010 an important SMS alert was sent to the old mobile No. which had already been de-registered. Further, that the amount withdrawn of Rs.1,62,800/- had been transferred to an account belonging to one Mr. Shakir Isha Quraishi with ICICI Account No.003201021669 and who had used IP Addresses of 82.128.16.10 and 92.46.220.21 and that his mobile No. was 9029922360. The petitioner has also been informed that Mr. Shakir Isha Quraishi had given the amount to one Mr. Chetan whose contact No. was 9321193011.



4. The petitioner concluded that he has suffered a wrongful loss of Rs. 1,62,800/- due to the unauthorized access of his savings Bank Account at the Anna Nagar Branch of ICICI inspite of not having compromised his password and other details. He is of the opinion that this wrongful access to his electronic bank account resulting in a loss to him was due to inadequacy of the bank to provide safety and security to his savings bank account. He has also stated that as the alleged fraudster is an account holder of ICICI bank, it was the responsibility of the bank to pursue the case. Also, that as the bank had failed to act in the interest of the customer; they were liable to compensate the customer.

Respondent:

5. The respondent in response to the petitioner's statement alleging that ICICI bank was responsible for this wrongful loss has stated that as the respondents are mainly carrying on business at Mumbai this complaint should have been dealt with at Mumbai and that the complainant has fallen victim to the alleged fraudulent debit transaction as he has inadvertently clicked on a phishing mail and that the complainant should follow up on the Police complaint filed before the Cyber Crime Branch. The respondent has also stated that the Adjudicating Officer can adjudicate under Section 43 of the Act only against the fraudster namely the 5th respondent. The respondent has also stated that the complainant has failed to adequately follow up on the complaint before the Police. The respondent has also stated that the Adjudicating Officer is vested with powers to try the complaint summarily and has no powers to conduct a trial.

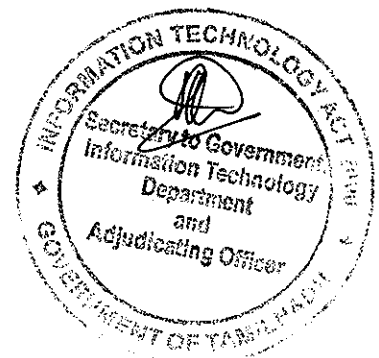


as in a Civil Court. In stating this, the petitioner has drawn attention to Section 58 (1) that provides for the jurisdiction of the Adjudicating Officer in processing a complaint based on the principles of natural justice and not being bound by the procedures laid down by the Code of Civil Procedures 1908.

6. The respondent has also provided information that it has circulated through its website and ATM locations on precautions that need to be taken by a customer. This includes an elaborate list of do's and don'ts and instruction on phishing mails. Instructions have also been provided on frequent changing of passwords and other computer safety measures. The respondent has also denied allegations that they had not exercised due diligence in compliance with KYC requirements and that in opening the account of Mr. Shakir Isha Quraishi all KYC norms had been followed. Also, that the IP Addresses of the two transactions were said to be originated from Nigeria and Kazakhstan and that as the e-mails had originated from a different server set, the bank had no control over the origin of the e-mails. The respondent concluded that the bank was not responsible for this situation and therefore requested that the complaint be dismissed.

Judgment:

7. The initial part to be addressed is with regard to the maintainability of the petition that has been submitted. The petitioner who has an account with the respondent bank had put his full trust on the system provided in order to make transactions and in the process has incurred wrongful loss to his income. He has



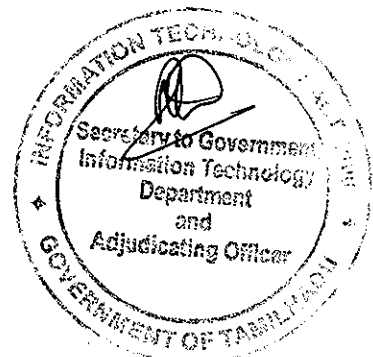
appealed under Section 46 which provides for provision to adjudicate over issues relating to Chapter 9 of the Information Technology Act, 2000. Section 43 of the I.T. Act that is relevant to the issue being discussed is quoted below and in particular the relevant sub sections to the incident in question:

Section 43 of the IT Act reads as 'Penalty and Compensation for damage to computer, computer system, etc.: - If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network, -

- a) accesses or secures access to such computer, computer system or computer network or computer resource;
- b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
- g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;
- h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network.

Along side this, Section 85 (1) of the IT Act reads as follows:

(1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder is a company, every



person who, at the time the contravention was committed was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly;

Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

(2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention any shall be liable to be proceeded against and punished accordingly.

8. The sections quoted herein of Section 43 and Section 85 of the IT Act provides sufficient scope to conclude that when an institution and in this case a banking institution, which has provided a framework for monetary transactions, with a provision for depositing and withdrawing individual finances utilizing an IT platform that has now been alleged to have failed to prevent a wrongful loss and also to have failed to prevent another customer of the bank from being party to



the wrongful loss and who has prevented unauthorized access and leading to data extraction that has led to loss – it can be safely concluded that allegation of such an incident falls within the adjudication provision of the IT Act, 2000. Therefore, the petition submitted before the Adjudicating Officer by the Petitioner is maintainable within the provisions of this Act. Also, the petitioner holds an account at the ICICI Bank, Anna Nagar Branch, Chennai, Tamil Nadu from which he has suffered wrongful loss and therefore has rightly approached the Adjudicating Officer for Tamil Nadu.

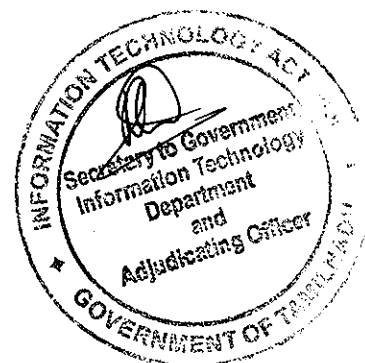
9. Secondly, the financial system of making online transactions on the IT platform in the ICICI Bank and agreed to by both the petitioner and the respondent is as follows:

a) Each customer is provided a login ID and a password which is changed immediately by the customer to ensure confidentiality.

b) On entering into the customer's account, he is provided a fund transfer option by which he can transfer funds (i) within the account (if he has multiple accounts), or / and (ii) within ICICI branches or / and (iii) to an account in non-ICICI branch.

c) On choosing one of the above options, the customer provides the name of the beneficiary, account No. and the name of the bank.

d) Following the above step, a Unique Registration Number (URN) is sent by the bank to the mobile phone number of the customer which is registered with the bank.



e) The customer then enters the URN number on the slot provided for this purpose and confirms the transaction.

f) The beneficiary is then added on to the beneficiary list of the customer.

g) Following this, the fund transfer option is exercised with the payees name and amount.

h) Following the above step, the bank IT application requests for a transaction password which is different from the user ID password.

i) Provision is then made to enter a grid value that changes every time the customer enters his account domain. (Each debit card of the ICICI bank has a grid value statement that would show a double digit number against sixteen letters such as A to P. No two cards have the same value for each letter.) So, in one transaction, the grid value requested could be for ACP or JLN with the values changing for every card and the customer is required to fill in the values attached to those individual letters found on the rear part of the debit card.

j) After the above procedure, the payment is released and the SMS is sent to the customer's mobile number thereby completing the transaction.

This clearly indicates that an elaborate system of checks and balances have been brought into place to ensure that the customer's identity is established before making a transaction. However, the system also indicates that availability of password information in two stages is necessary to transfer funds. This elaborate system also indicates that some degree of cooperation, connivance or



total inadequacy is necessary by the customer or the personnel in the bank if the system is to be exploited in order to result in wrongful loss to the customer.

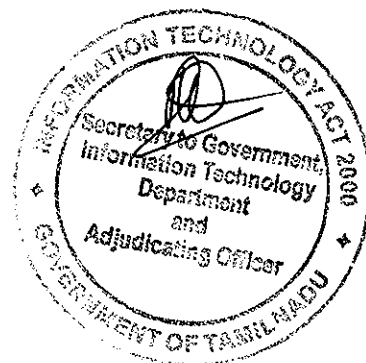
10) Thirdly, during the arguments in this case, it surfaced that the mobile phone number played a key role and this has to be examined. The customer had left for the USA to work there for a period of time. During this period, he had contacted the ICICI branch to inform them that he had surrendered his mobile number. He was then informed that it was not possible to change a mobile number over the telephone and that he had to go in person to record the same at an ICICI branch. As he was unable to visit an ICICI branch at the city in the USA that he was working in the customer had not been able to do this. Subsequently, after a period of three months, as is the provision to do so, the surrendered mobile card had been reallocated to someone else in India. Apparently, this mobile sim card which was now being utilized by 'someone else' had played an important role in completing the transaction resulting in wrongful loss to the customer. The ICICI bank on their part was of the opinion that it was the fault of the customer not to have followed up and ensured that the mobile number was deregistered.

It must be observed that there is a strong suspicion about how a mobile sim card that had been surrendered on a routine basis could find itself in the hands of another who in turn managed to secure the requisite passwords that ultimately resulted in the wrongful loss to the customer. It is also observed that the immediate beneficiary was another customer of the ICICI and who was based



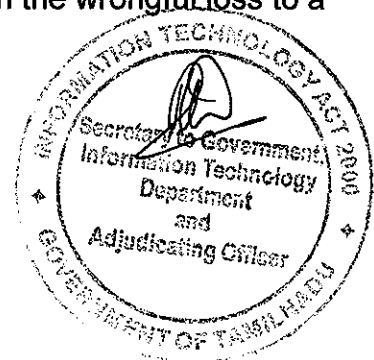
in Mumbai. There appears to be a lack of foresight on the part of the bank to have ensured a customer-friendly procedure at any time that a sim card is to be surrendered or replaced. Also, the bank has failed to provide such a system that would block usage of the mobile number at short notice by insisting on the physical appearance of the customer which has in this case led to the damage. Some banks have a basic and clever authentication system in order to identify the customer over telephone and even this was not in place. The respondent bank has also not been able to fully explain how a reallocated mobile number could manage to fit the password pieces together both at the login stage and the transaction stage. The needle of suspicion points to some degree of connivance or cooperation of persons familiar with the banking systems within the bank.

11. Fourthly, in this case, the wrongful beneficiary who claims to have passed on money that was withdrawn from the customer's account into his account was actually a customer of the ICICI bank. The Reserve Bank of India have issued instructions on the Know Your Customer (KYC) norms by which customers need to be properly reviewed and assessed to prevent banks from being used intentionally or unintentionally by criminal elements for money laundering. Also, as observance of KYC norms will enable banks to manage their risks in a prudent manner. Several circulars have been issued to highlight the crucial role in banks following the KYC norms and this has been published in the Reserve Bank of India website.



In fact very stringent measures have been determined by Reserve Bank of India to curb money laundering and by the Bank's own admission of this being money laundering case it is disheartening to note that the Respondent Bank has failed to act in a decisive manner. In fact in RBI-2004-05/284 BOD.NO.AML.BC.58/14.01.001/2004-05 dated Nov 29 2004 RBI has clearly outlined several measures related to KYC norms and has even provided for cancellation of an account holder if there appears to have been an attempt at money laundering. In this case, there has been no such step by the bank. With the information provided in this case, the customer in whose account the money was first drawn into and who claims that this was given to a third party, there has been poor follow up by the bank on there own customer who claims to have played an in-between role. The bank has not being forthcoming on the nature of character verification and other KYC norms followed on this customer namely Thiru Shakir Isha Quarishi. This clearly indicates a lack of commitment and adherence to the basic KYC norms required of a banking institution.

12. Fifthly, there is an obvious lack of concern from the bank in attending to an incident wherein one of their own customers has been affected by a serious wrongful loss that was caused by another customer of the same bank. The entire responsibility for follow up has been left to the customer with no assistance from the bank. The respondent bank has addressed itself of being devoid of any responsibility to approach the Police on the wrongful and fraudulent use of their own Information Technology framework that has resulted in the wrongful loss to a



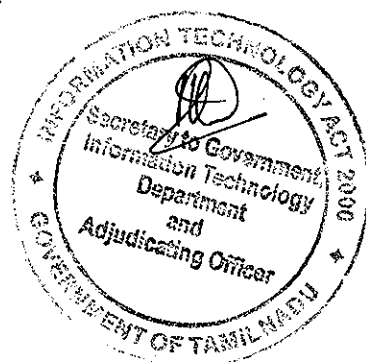
customer. The Respondent Bank has preferred to accept the statement of the customer benefiting from this illegal transaction by remaining non-committal on furthering investigation in the matter. Such lack of deeper investigation has been evident by the Respondent Bank. Although the two IP addresses in the transaction are from foreign countries, an Indian ICICI account holder has been the key beneficiary. The indifference of the bank to follow up on their own customer who exploited another customer utilizing the IT Banking System of the Bank is puzzling and is indicative of a deeper conspiracy in place.

13. Considering all the factors above, it is concluded that the respondent bank has failed to establish due diligence in preventing the unauthorized access into the petitioner's account in this case and in providing adequate checks and safeguards that would have given the much needed security to the account of the customer. The KYC norms have apparently not been adhered to and there is a complete lack of concern to the customer who had placed his trust on the bank and the IT framework provided by the respondent.

14. With regard to the quantum of compensation, Section 47 (b) of the IT Act, 2000 has stated that due regard shall be had to the quantum of loss suffered by the petitioner.

a) In this case, the petitioner has suffered a monetary loss of Rs.1,62,800/-.

b) If this amount is computed at an interest rate of 12% per annum till the date of filing of case, an amount of Rs.17,200/- is due to the petitioner.



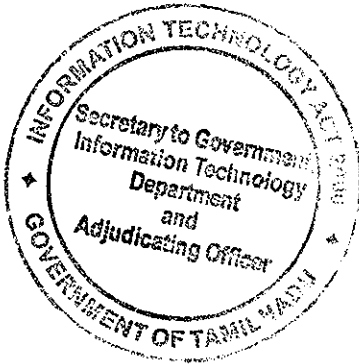
c) Further, the total fee paid by the petitioner as statutorily applicable is Rs.27,850/-.


d) In addition to the above, the petitioner needs to be compensated for all the difficulties that he has had to encounter on account of this unfortunate incident and this is computed on a lumpsum basis of Rs.30,000/-.

Therefore the total amount expected of the respondent bank to pay the petitioner is Rs.2,37,850/- (Rs.1,62,800 + 17,200 + 27,850 + 30,000) and this should be paid within 60 days from the date of issue of the judgment.

Thus, the respondent bank namely ICICI in the instant case is directed to pay a total sum of Rs.2,37,850/- (Rupees two lakhs thirty seven thousand eight hundred and fifty only) to the petitioner within 60 days from the date of issue of this judgment.

The application for adjudication is ordered with the above direction.




(P.W.C.DAVIDAR)
Adjudicating Officer and
Principal Secretary to Government,
Information Technology Department,
Government of Tamil Nadu.